AMENDMENTS TO THE CLAIMS

This listing of Claims shall replace all prior versions, and listings, of claims in the application:

LISTING OF CLAIMS:

1. (Currently Amended) A processor with secure cryptographic capabilities, said processor comprising:

a digital secret ~~that comprises~~ comprising a secret key used in a key-based cryptographic process, wherein said digital secret is ~~internally accessible~~ stored only within said processor, and wherein said digital secret is operable to be used exclusively by said processor for both encryption and decryption;

a cryptography engine for performing said key-based cryptographic process internally within said processor, said cryptography engine ~~coupled~~ operable to access said digital secret; and

internal memory coupled to said cryptography engine for supporting said key-based cryptographic process.

2. (Original) The processor of Claim 1 further comprising an internal bus for facilitating secure communication between said cryptography engine, said digital secret, and said internal memory within said processor.

3. (Original) The processor of Claim 1, wherein said digital secret is securely confined within said processor.

4. (Currently Amended) The processor of Claim 1, wherein said internal memory comprises[[:]] microcode for implementing said key-based cryptographic process on data within said processor, and wherein said internal memory is

operable to perform state tracking associated with said key-based cryptographic process.

5. (Original) The processor of Claim 1, wherein said internal memory securely stores intermediate data created within said key-based cryptographic process.

6. (Original) The processor of Claim 1, further comprising:

a cryptography unit comprising a functional unit within said processor for securely executing said key-based cryptographic process internally within said processor, wherein said cryptography unit comprises:

said digital secret;

said cryptography engine; and

said internal memory.

7. (Original) The processor of Claim 1, wherein said key-based cryptographic process comprises:

a key-based encryption process; and

a key-based decryption process.

8. (Original) The processor of Claim 1, wherein said processor comprises:

a secure hardware environment providing core processing functionality; and

a secure software environment coupled to said secure hardware environment, said secure software environment generating executable instructions that are sent to said secure hardware environment for processing, said secure hardware environment in combination with said secure software

environment providing processor capability, and wherein said secure hardware environment is accessible only through said secure software environment.

9. (Original) The processor of Claim 1, wherein said digital secret is unique to said processor and is permanently and physically manifested within said processor.

10. (Currently Amended) A processor with cryptographic capabilities, said processor comprising:

a secure cryptography unit, wherein said cryptography unit internally provides secure cryptographic capabilities as a functional unit within said processor, said cryptography unit comprising:

a cryptography engine for performing a key-based cryptographic process;

a digital secret ~~coupled~~ exclusively accessible to said cryptography engine ~~and accessible only by said cryptography engine~~, wherein said digital secret comprises a secret key used in said key-based cryptographic process, and wherein said secret key is operable to be used exclusively by said processor for both encryption and decryption; and

internal memory coupled to said cryptography engine for supporting said key-based cryptographic process.

11. (Original) The processor of Claim 10, wherein said key-based cryptographic process comprises:

a key-based encryption process; and

a key-based decryption process.

12. (Original) The processor of Claim 10, wherein said processor comprises a very long instruction word (VLIW) processor.

13. (Original) The processor of Claim 10, wherein said processor comprises:

a secure hardware environment providing core processing functionality; and

a secure software environment coupled to said secure hardware environment, said secure software environment generating executable instructions that are sent to said secure hardware environment for processing, said secure hardware environment in combination with said secure software environment providing processor capability, and wherein said secure hardware environment accessible only through said secure software environment.

14. (Original) The processor of Claim 10, wherein said digital secret is unique to said processor and is permanently and physically manifested within said processor.

15. (Original) The processor of Claim 10, wherein said digital secret comprises:

a plurality of fusible links to manifest said digital secret by permanently setting a binary state in each of said plurality of fusible links.

16. (Original) The processor of Claim 10, wherein said digital secret comprises a random number that is generated from an HMAC algorithm implemented on testing data associated with fabrication of said IC chip.

17. (Original) The processor of Claim 16, wherein said testing data comprises:

wafer test data; and

die test data.

18. (Original) The processor of Claim 10, wherein said secure cryptography unit comprises a fully integrated circuit within said processor.

19. (Currently Amended) The processor Claim 10, wherein said digital secret and said internal memory are fully integrated with said cryptography engine to facilitate communication without ~~requiring~~ use of a bus ~~and which is not susceptible to malicious attack~~.

20. (Original) The processor of Claim 10, wherein said key-based cryptography process comprises a Triple Data Encryption Algorithm (TDEA or Triple DES) cryptography process.

21. (Currently Amended) A processor with secure cryptographic capabilities, said processor comprising:

a secure hardware environment providing core processing functionality, wherein said secure hardware environment comprises:

a secure cryptography unit~~, wherein said cryptography unit internally provides~~ for providing secure cryptographic capabilities as a functional unit within said secure hardware environment, wherein said secure cryptography unit is operable to facilitate performance of a key-based cryptographic process performed exclusively by said processor,

and wherein said key-based cryptographic process comprises encryption using a digital secret and decryption using said digital secret.

22. (Original) The processor of Claim 21, further comprising:

a secure software environment for accessing said secure hardware environment, said secure software environment generating executable instructions that are sent to said secure hardware environment for processing, said secure hardware environment in combination with said secure software environment providing processor capability.

23. (Currently Amended) The processor of Claim 21, wherein said secure cryptography unit comprises:

a cryptography engine for performing ~~a~~ said key-based cryptographic process;

~~a~~ said digital secret ~~coupled~~ accessible exclusively to said cryptography engine ~~and accessible only by said cryptography engine~~, wherein said digital secret comprises a secret key used in said key-based cryptographic process; and

internal memory coupled to said cryptography engine for supporting said key-based cryptographic process and for performing state tracking associated with said key-based cryptographic process.

24. (Original) The processor of Claim 23, wherein said internal memory securely stores intermediate data created within said key-based cryptographic process.

25. (Original) The processor of Claim 21, wherein said secure cryptography unit comprises a fully integrated circuit within said processor.

26. (Currently Amended) The processor of Claim 23, wherein said secure cryptography unit comprises a fully integrated circuit within said processor to facilitate communication between said cryptography engine, said digital secret and said internal memory without ~~requiring~~ use of a bus.